

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*INFORMATION ASSOCIATED WITH THE ACCOUNT OF  
TUTTDEVIN2110@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE, INC.Case No. **1:20-MJ-00074**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A-4

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B-4

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

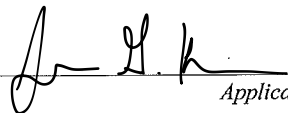
- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2252(a)(2) and (b)(1)	Distribution & receipt of a visual depiction of a minor engaged in sexually explicit conduct
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	Possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct

The application is based on these facts:

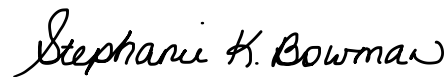
SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.☐ Delayed notice of        days (give exact ending date if more than 30 days:                     ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.*Applicant's signature*

SPECIAL AGENT JASON G. KEARNS, HSI

*Printed name and title*

Sworn to before me and signed in my presence.

Date: Jan 30, 2020City and state: CINCINNATI, OHIO*Judge's signature*

HONORABLE STEPHANIE K. BOWMAN

*Printed name and title*

**ATTACHMENT A-4**

**Property to Be Searched**

This warrant applies to information associated with **TUTTDEVIN2110@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Way, Mountain View, California.

**ATTACHMENT B-4**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, Inc. (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.
- g. Notwithstanding Title 18, United States Code, Section 2252A, Google may disclose responsive data, if any, by delivering encrypted files through Google’s Law Enforcement Request System (LERS).

**II. Information to be seized by the government**

a. All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 2252 including the following:

1. Communications about or reflecting the transportation, possession, receipt, distribution, or production of child pornography;
2. Communications that reveal, or provide leads to identify the account owner and additional co-conspirators;
3. Documents, photographs, digital files, or other electronic media, attached or otherwise stored electronically, related to any of the above-listed matters.
4. Any child pornography or child erotica; and
5. Any communications concerning dropbox.

Pursuant to 18 U.S.C. §§ 2256(8), Child Pornography is defined as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

Pursuant to 18 U.S.C. §§ 2256(1), the term “minor,” as “any person under the age of eighteen.”

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Jason G. Kearns a Special Agent (“SA”) with Homeland Security Investigations, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security, Homeland Security Investigations (“HSI”) since 2005 and am currently assigned to Cincinnati. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. I have gained experience through training at the Federal Law Enforcement Training Center and everyday work relating to conducting these types of investigations. I have also participated in the execution of numerous search warrants involving child exploitation and/or child pornography offenses. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2252A, and I am authorized by law to request a search warrant.

2. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2252/2252A (Possession, Receipt, & Distribution of Child Pornography) have been committed by Devin Michael Tutt (DOB XX/XX/1999). This Affidavit is submitted in support of Applications for search warrants for the following:

- a. The Google account **TUTTDEVIN3621@GMAIL.COM**; as more fully described in Attachment A-1. The items to be searched for and seized are described more particularly in Attachment B-1.

- b. The Dropbox account **TUTTDEVIN3621@GMAIL.COM (UID 535539994)**; as more fully described in Attachment A-2. The items to be searched for and seized are described more particularly in Attachment B-2.
- c. The Dropbox account **TUTTDEVIN2110@GMAIL.COM (UID 613463392)**; as more fully described in Attachment A-3. The items to be searched for and seized are described more particularly in Attachment B-3.
- d. The Google account **TUTTDEVIN2110@GMAIL.COM**; as more fully described in Attachment A-4. The items to be searched for and seized are described more particularly in Attachment B-4.

Upon receipt of the information described in Section I of the respective Attachment B (1-4), government-authorized persons will review that information to locate the items described in Section II of the respective Attachment B (1-4).

3. The statements in this affidavit are based on my investigation of this matter as well as information conveyed to me by other law enforcement officers. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2252(a)(2) and (b)(1) (distribution and receipt of a visual depiction of a minor engaged in sexually explicit conduct); 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (possession of and access with intent to view a visual depiction of a minor engaged in sexually explicit conduct).

**STATUTORY AUTHORITY**

4. As noted above, this investigation concerns alleged violations of the following:

a. Title 18, United States Code, Sections 2252(a)(2) and (b)(1) prohibit any person from knowingly receiving or distributing, or attempting or conspiring to receive or distribute, any visual depiction using any means or facility of interstate or foreign commerce, or that has been mailed or shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproducing any visual depiction for distribution using any means or facility of interstate or foreign commerce, or in or affecting interstate or foreign commerce or through the mails, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

b. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

### **DEFINITIONS**

6. The following definitions apply to this Affidavit and Attachment B:

a. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. “Child erotica,” as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.



d. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet service providers (ISPs) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

e. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

f. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

h. “Mobile applications,” as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

i. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

j. “Remote Computing Service” (“RCS”), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

k. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

l. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

m. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

n. Whois: A “Whois” search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record

for a particular IP address or domain name will list a range of IP addresses that that IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.345.67.0– 12.345.67.99 and list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.345.67.0– 12.345.67.99.

### **PROBABLE CAUSE**

7. Based on the instant investigation as described further herein, there is probable cause to believe that Devin Michael Tutt has engaged in the possession and receipt of child pornography.

8. On November 22, 2019, your affiant met with Detective Shane Hatfield with the Prebble County Sheriff's Office (PCSO) in Eaton, Ohio. Detective Hatfield advised that he was investigating Tutt for the rape of several minor females. During the course of his investigation, Detective Hatfield executed a state search warrant for Devin Tutt's Apple iCloud account, associated with the emails of tuttdevin@icloud.com, devintutt36@icloud.com, devintutt21@icloud.com between the dates of 11/5/2017 and 8/6/2019. Your affiant reviewed the information provided by Apple in regards to the aforementioned search warrant and observed images of child pornography located in the iCloud account. The images of child pornography included toddlers, bondage, and sadomasochistic material. Below are four of the file paths to the child pornography with descriptions of the images.

Devin's iPad (iPad Air 2)/applications/com.kik.chat/Documents/convothumbs/0643cd79-66f8-4a5e-8ffb-156cdb55c0ba

The picture is a prepubescent female lying on her back completely naked. There is a male kneeling on the bed with his penis inserted into her vagina.

Devin's iPad (iPad Air 2)/applications/group.com.kik.chat/cores/private/010b4b71634546dc8c535ebcdbbdf7c4/a

ttachments/0f46ae5b-0d0e-49fb-ab72-fd5a1cf69128/0f46ae5b-0d0e-49fb-ab72-fd5a1cf69128\_embedded\_1.jpg

The picture is of two prepubescent females lying on their back with their legs in the air. They are wearing bras and nothing else on the top half of their body. One of the prepubescent females, her panties are pulled up to almost her knees and her hands are spreading her vagina. The other prepubescent females hands are pulling her panties to the side exposing her vagina.

Devin's iPad (iPad Air 2)/applications/com.kik.chat/Documents/convothumbs/21201de1-31a7-4b4e-aef2-925b2d7511c5

The picture is of a prepubescent female completely naked kneeling on the floor. There is a white gag in her mouth, her legs are bound to chairs behind her, and her wrists and arms are also bound.

Devin's iPad (iPad Air 2)/applications/com.kik.chat/Documents/convothumbs/8762c835-a400-4684-a8bb-e82df4b47cd7

The picture is of a prepubescent female. She is wearing a blue striped shirt and nothing below the waist. Her legs are in the air and it appears that a male penis is being inserted into her anus.

9. The affiant also observed links to a Dropbox account with User ID (UID):

535539994. The links were indicative of child pornography movies. The affiant was unable to view the videos because they were stored at Dropbox. The following were several of the links:

Dropbox user: 535539994/Spotlight/! NEW ! 2009 --7yo neighbour.wmv<sup>1</sup>  
Dropbox user: 535539994/Spotlight/! New ! (pthc) (kinderkutje) 11yo Bianca Sales.wmv<sup>2</sup>  
Dropbox user: 535539994/Spotlight/!!! NEW Pthc - 11yo Evelyn 2010!!!.mp4

10. On or about November 22, 2019, a Preservation Letter was submitted to Dropbox for account User ID: 535539994.

---

<sup>1</sup> 7yo is an abbreviation for 7 year old.

<sup>2</sup> PTHC is commonly utilized in the trading of child pornography. PTHC is an acronym for Pre-Teen Hard Core. 11yo is an abbreviation for 11 year old.

11. On December 3, 2019, a Federal Grand Jury Subpoena was issued and served on Dropbox. It requested subscriber information related to Dropbox User 535539994.

12. On December 17, 2019, Dropbox responded to the aforementioned Grand Jury Subpoena. Dropbox provided the following information:

Name: Devin Tutt

Email: tuttdevin3621@gmail.com

User ID: 535539994

Joined: Fri, 12 Feb 2016 02:15:15 GMT

Current Account Status: Active

Subscription Status: Free

13. On or about December 18, 2019 a preservation letter was submitted to Google for the TUTTDEVIN3621@GMAIL.COM account.

14. Your affiant continued to review the Apple iCloud search warrant return. The affiant discovered that there was another Dropbox account that appeared to contain child pornography. The affiant observed the following links to videos which contained names that were indicative of child pornography. The affiant was unable to view the videos because they were stored at Dropbox.

DropBox user: 613463392/Spotlight/12yo and dog\_x264.mp4<sup>3</sup>

DropBox user: 613463392/Spotlight/2014-05 - VID 20120902 bj 3yo.avi<sup>4</sup>

15. On or about January 6, 2020, a Preservation Letter was submitted to Dropbox for account User ID: 613463392.

---

<sup>3</sup> 12yo is an abbreviation for 12 year old.

<sup>4</sup> Bj 3yo is a reference for oral sex with a 3 year old.

16. On January 22, 2020, a Federal Grand Jury Subpoena was issued and served on Dropbox. It requested subscriber information related to Dropbox User 613463392.

17. On January 23, 2020, Dropbox responded to the aforementioned Grand Jury Subpoena. Dropbox provided the following information:

Name: Devin Tutt

Email: tuttdevin2110@gmail.com

User ID: 613463392

Account Creation Date: 2016-10-13 06:14:32 UTC

Current Account Status: Active

Subscription Status: Free

#### **BACKGROUND ON CHILD PORNOGRAPHY AND THE INTERNET**

18. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.
- b. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone or external media in most cases.

c. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

#### **BACKGROUND CONCERNING EMAIL**

19. In my training and experience, I have learned that Google, Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Google, Inc. allows subscribers to obtain email accounts at the domain name Gmail.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

20. A Google subscriber can also store with the provider files in addition to emails such as pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google, Inc.

21. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

22. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.



23. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

24. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further

indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

### **BACKGROUND CONCERNING DROPBOX**

25. Dropbox is a service that allows its users to store files on Dropbox's servers. According to Dropbox's privacy policy, at <https://www.dropbox.com/privacy>, Dropbox collects and stores "the files you upload, download, or access with the Dropbox Service," and also collects logs: "When you use the Service, we automatically record information from your Device, its software, and your activity using the Services. This may include the Device's Internet Protocol ("IP") address, browser type, the web page visited before you came to our website, information you search for on our website, locale preferences, identification numbers associated with your Devices, your mobile carrier, date and time stamps associated with transactions, system configuration information, metadata concerning your Files, and other interactions with the Service. "Dropbox is a free service that lets you bring all your photos, docs, and videos anywhere. This means that any file you save to your Dropbox will automatically save to all your computers, phones and even the Dropbox website."

26. The Dropbox Law Enforcement Handbook also states that Dropbox maintains IP addresses for web-based logins and the last-seen IP address of linked computers. IP address information is typically maintained for 6 months, but this may be extended with a preservation request. IP addresses of specific actions within a Dropbox account, such as uploads and deletions, are not available. IP address login information is recorded when a user logs in to Dropbox through

the website. Like many online services, Dropbox sometimes uses cookies stored on a browser so that a user may not need to sign in every time they visit the website. Additionally, if a user is accessing files in their Dropbox account from a desktop or mobile application, that access may not be logged by Dropbox.

27. In general, providers like Dropbox ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, e-mail addresses, and, for paying subscribers, a means and source of payment (including any credit or bank account number). Providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account, and other log files that reflect usage of the account. In addition, providers often have records of the IP addresses used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account. Additionally, providers like Dropbox commonly keep records about whether the email address used to create the account was verified. The verification of the email address associated with the account can occur several ways, one is by sending an email to the address asking the account user to confirm it created the dropbox account.

28. In some cases, account users will communicate directly with a provider about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Providers typically retain records about such communications, including records of contacts

between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO RECEIVE, POSSESS,  
AND/OR ACCESS WITH INTENT TO VIEW CHILD PORNOGRAPHY**

29. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Such individuals almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape

recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

e. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.<sup>5</sup>

---

<sup>5</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology"); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

f. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

g. Such individuals prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if Tutt uses a portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in his home.

30. Based on the following, I believe that Devin Michael Tutt likely displays characteristics common to individuals who receive, possess or access with intent to view child pornography.

31. Based on the forgoing, I request that the Court issue the proposed search warrants. Because the warrant will be served on Dropbox.com and Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

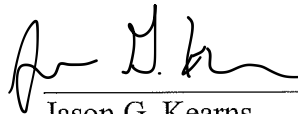
#### **REQUEST FOR SEALING OF AFFIDAVIT**

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because

their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

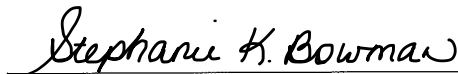
**CONCLUSION**

33. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachments B1 – B4, are located at the locations described in Attachments A1 – A4. I respectfully request that this Court issue a search warrant for the locations described in Attachment A1 - A4, authorizing the seizure and search of the items described in Attachment B1 – B4.



Jason G. Kearns  
Special Agent  
Homeland Security Investigations

Sworn and subscribed before me this 30 th day of January, 2020.



HONORABLE STEPHANIE K. BOWMAN  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A-4**

**Property to Be Searched**

This warrant applies to information associated with **TUTTDEVIN2110@GMAIL.COM** that is stored at premises owned, maintained, controlled, or operated by Google Inc., a company headquartered at 1600 Amphitheatre Way, Mountain View, California.



**ATTACHMENT B-4**

**Particular Things to be Seized**

**I. Information to be disclosed by Google, Inc. (the “Provider”)**

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails associated with the account, including stored or preserved copies of e-mails sent to and from the account, draft e-mails, the source and destination addresses associated with each e-mail, the date and time at which each e-mail was sent, and the size and length of each e-mail;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;
- e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.
- f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.
- g. Notwithstanding Title 18, United States Code, Section 2252A, Google may disclose responsive data, if any, by delivering encrypted files through Google’s Law Enforcement Request System (LERS).

**II. Information to be seized by the government**

a. All information described above in Section I that constitutes fruits, evidence and instrumentalities of 18 U.S.C. § 2252 including the following:

1. Communications about or reflecting the transportation, possession, receipt, distribution, or production of child pornography;
2. Communications that reveal, or provide leads to identify the account owner and additional co-conspirators;
3. Documents, photographs, digital files, or other electronic media, attached or otherwise stored electronically, related to any of the above-listed matters.
4. Any child pornography or child erotica; and
5. Any communications concerning dropbox.

Pursuant to 18 U.S.C. §§ 2256(8), Child Pornography is defined as “any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where – (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; . . . or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.”

Pursuant to 18 U.S.C. §§ 2256(1), the term “minor,” as “any person under the age of eighteen.”

b. Records relating to who created, used, or communicated with the account or identifier, including records about their identities and whereabouts.